12-5-2006

Social Engineering and its Impact via the Internet

Matthew J. Warren
Deakin University

Shona Leitch
Deakin University

DOI: 10.4225/75/57b661be34775
4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006

Social Engineering and its Impact via the Internet

Matthew J. Warren and Shona Leitch

School of Information Systems,
Faculty of Business and Law,
Deakin University,
Geelong, Victoria, Australia, 3217

mwarren@deakin.edu.au and shona@deakin.edu.au

Abstract

Historically social engineering attacks were limited upon a single organisation or single individual at a time. The impact of the Internet and growth of E-Business has allowed social engineering techniques to be applied at a global level. The paper will discuss how new social engineering techniques are being applied and puts forward a conceptual model to allow an understanding of how social engineering attacks are planned and implemented against E-Business activities.

Keywords

Social Engineering, Internet and Blogging.

INTRODUCTION

Decisions are based on information or knowledge. The decision-maker naturally assumes that it reflects reality. Yet data, which is used to create information, is easily manipulated, and the context for information can be changed to influence knowledge derived from the situation. The use of deception is not new, but the advent of electronic information systems has made its potential more pervasive. This paper investigates the dilemma the information management function faces in ensuring the integrity of the data supplied, the information derived, and the knowledge created from their systems.

E-Business is built on the concept of trust. "Trust no one. In today's volatile global markets, deception, misrepresentation, and outright dishonesty are among the few constants" (Rothkopf, 1999). E-Business relies on the integrity of its data stored in digital format. Woolford (1999) emphasises the criticality of authenticity and data integrity. The effectiveness of E-Business is determined by the security associated with its systems. Transaction and stored data must have high integrity. Internal data such as transport, accounting transaction, and client details are often transferred on open networks. Data for external consumption such as marketing materials as well as transaction interfaces are also accessible via the Internet. This makes them vulnerable to attack from anywhere in the world.

DECEPTION

Although the term 'reality' is used in this paper, 'truth' is not. Previous research (Warren and Hutchinson, 2001) illustrate the illusion of 'truth'. Reality is less emotive, and here, is meant to describe the perceived truth of individuals.

Deception has been used since the dawn of time to gain advantage. The purpose of deception is to create an illusion, which somehow benefits the perpetrator. By its nature, a deception should not be discovered to be successful. Deception is the deliberate manipulation of data or a situation to produce a desired reality. Thus, decisions and behaviours of the target are changed to the benefit of the attacker.

Organisations and the people in them have always been prone to deception. The modern electronic organisation has both people and machines, which are vulnerable to false input. The increasing dangers of electronic attack by 'hackers' are well documented (for example, Denning, 1999; Schwartau, 1996). These dangers are increasing as attacks come not from individual hackers, but more organised competitors, criminal gangs, and foreign states (as the concept of economic warfare grows). You can now get more information about organisations or people with computers than by using any other means (Fialka, 1997), this is both the strength and weakness of the Information Society.

Table 1 lists some of the possibilities for deception. Of course, deception can be two fold: an organisation may perpetrate deception as well as being a victim of it.

Table 1: Examples of types of deception

TYPE OF DECEPTION	EXAMPLES
Masking	Stenography (Denning, 1999): hiding a message in other data.
Repackaging	Computer virus hiding in an existing program such as Trojan Horses.
Dazzling.	Encryption, codes. Sending false messages to make believe something a being carried out when it is not.
Mimicking	Web page looking like target's.
Inventing	Propaganda, public relations, advertising.
Decoying	Sending information so target directs effort to an activity beneficial to the attacker, e.g. by sending false market opportunities.

SOCIAL ENGINEERING

Social engineering is often perceived in a negative light due to the fact that it seems unacceptable to some to categorise social scientists as engineers (Turner, 2001) and the fact that manipulation, mind control and the underlying control of humans are the main features of this "science". It is in fact, these negative connotations that have caused distrust among society. It is the lack of social trust that has demoted the importance of social trust. Such trust can improve teamwork and knowledge sharing across countries and promote a democratic and stable world (Boslego, 2006). In an E-Business environment the absence or presence of such a trust can severely impact both positively and negatively the success of such a business. Our reasons as humans for choosing to trust or distrust "strangers" can be based on numerous things: our past experience, our upbringing, values and in the case of E-Business possibly even our level of understanding of technology. This type of attack which relies on trust is shown in Figure 1.

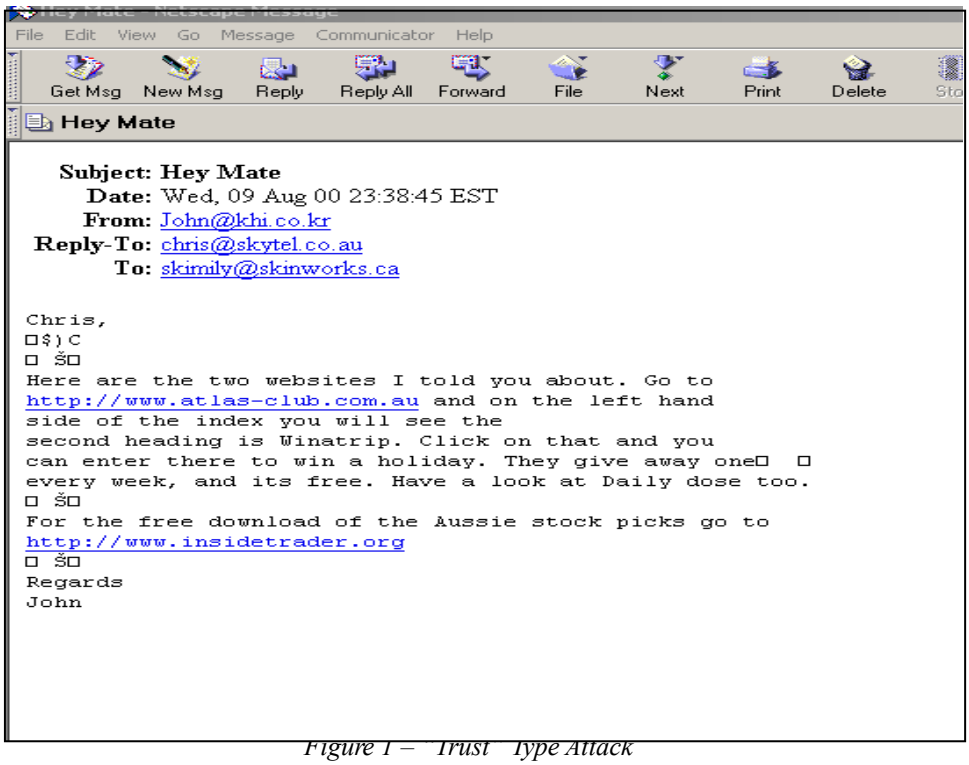

Figure 1 – "Trust" Type Attack

Gulati (2003) states that, "Social engineering is the 'art' of utilizing human behavior to breach security without the participant (or victim) even realizing that they have been manipulated." Standard hacking techniques have been around for decades, but the movement into using social engineering tricks to gain the "trust" of victims is on the increase. It could be suggested that for the hackers this is needed as more users become technologically savvy and especially those younger members of society who have experienced technology as part of their upbringing, and so the traditional methods hackers had of garnishing user information is not longer fruitful.

In a test carried out at a Texas University, over 90% of students parted with their authentication details after being sent spoofed e-mails and web pages, which looked like those of their University's IT department (Vijayan, 2005). This seems to suggest that using social engineering tricks is an effective mechanism for hackers to gain access to confidential information even in the groups in society who one would expect to be more cautious.

One of the most common of these tricks being encountered are e-mails manufactured to look like they are being sent from a major banking organisation (see Figure 2). As well as the fact it is common to trust someone with a particular logo or name, other human qualities come into play: the desire to be helpful and perhaps even the fear of getting into trouble. In the case of a banking organisation, a request to assist in an important survey or the "threat" that if you are not authenticated with 24 hours your account will be terminated, is often enough of a threat to provide a reaction in an individual.

The problem with these types of social engineering attacks is that they are based upon probability. In terms of Australia, there are a fixed number of major banks i.e. 5, this means any emails sent on behalf on a major Australian bank would have a 20% chance of reaching a customer of that bank. The problem comes when you look at a larger country such as USA or Europe where a larger number of banks exist. This means that sending out hoax emails would have a reduced chance of reaching customer. To overcome this, an attacker could resort to sending out emails to an even greater audience, hoping for success. This is shown in Figure 3, where a German email intended for a German bank customer would be sent to an Australian email address and the likelihood of that person being a German bank customer would be very remote.

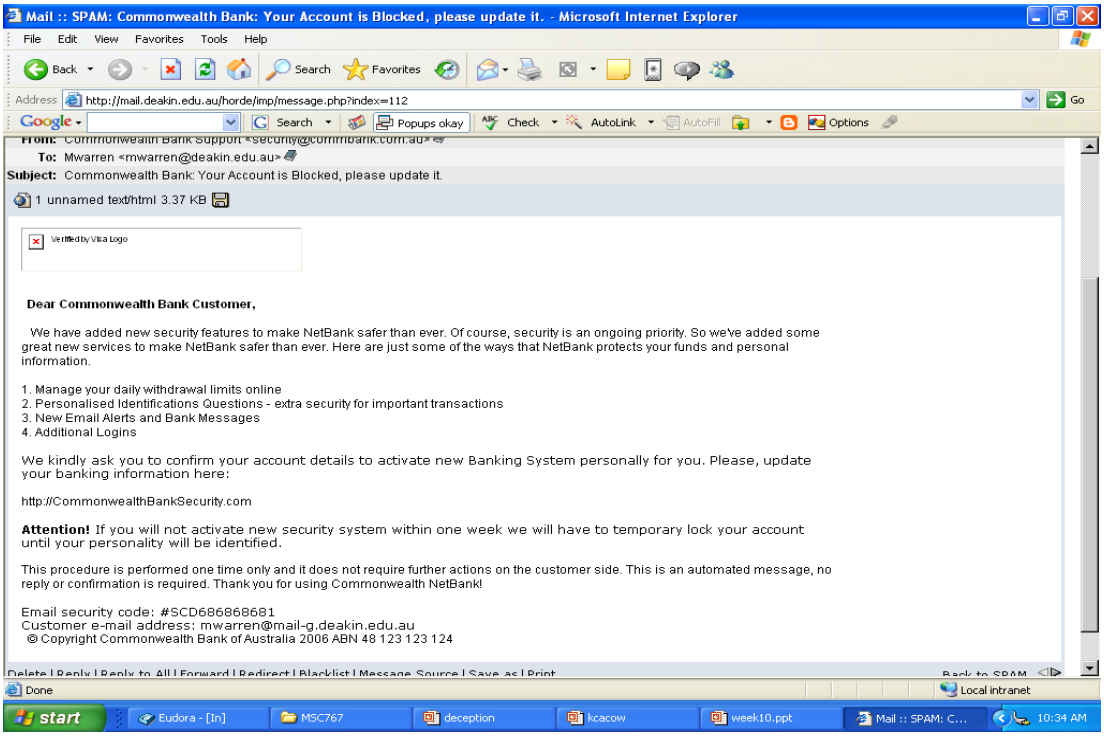

Figure 2 – Example of a spoof website for a banking organisation

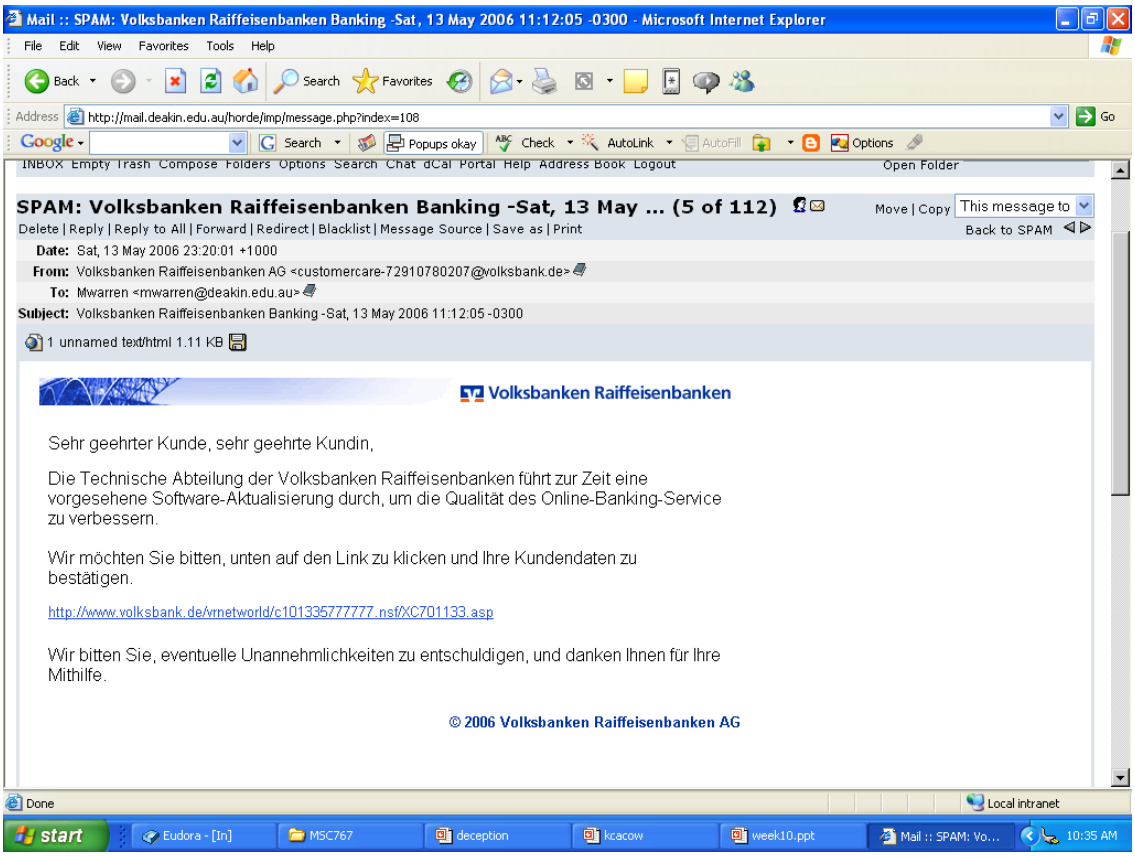

Figure 3 – Example of an unsuccessful spoof website

Most hackers engaging in the manipulation of users in this way follow a similar pattern in their planned exploitation, first starting by conducting their own research into the type of social engineering tricks that may work and on which targets. Then it is important for them to develop rapport and trust with the users, perhaps through fake web-sites (with highly realistic designs). They will then exploit the trust they have fostered and use the information for their own ends (e.g. obtaining money from bank accounts) (Mitnick, 2002).

Although this is one of the most common "ruses" being used currently, Mitnick, (2002) identifies a great many of these social engineering tricks that are being utilised:

- Manipulate lack of awareness of value of info.
- Posing as fellow employee, posing as employee of vendor, posing as a new. employee requesting help.
- Offering help if a problem occurs.
- Sending free software or patch to install.
- Using false pop-up window asking for log-in.
- Using insider lingo to gain trust.
- Offering a prize for registering web site with username and password.
- Modifying fax machine heading to appear to come from normal location.
- Asking for a file to be transferred to an apparently internal location.
- Getting voice mailbox set up for callbacks, making attacker seem internal.

As mentioned previously, hackers make good use of tactics when choosing their targets, usually organisations with a large number of employees, or who work on multiple facilities. What makes it even easier is the fact that most users (in organisations) have a lack of security training and no incident reporting or response plan (Mitnick, 2002).

By choosing the targets sensibly depending on the information that they are trying to obtain hackers can make life every easy for themselves, e.g. a receptionist may be targeted as they may be more likely to be unaware of the value of information (Mitnick, 2002).

BLOGGING

The use of blogging has become widespread allowing individuals around the world to share views and opinions via the Internet (Finn et al, 2005). The success relates to the fact that individuals can express their views and opinions about any subject or topic and people can respond to the views (Clyde, 2004). The problem relates to the fact that individuals can discuss any topic including their personal life and work life and experiences. From a security perspective this means that personal and work related information are discussed in an open forum. This information could be used to build up a profile about an individual's life. This information could be used in a social engineering context to attack an individual or organisation that they work for.

A major security risk is that the information is freely available via the Internet and there is no control on the distribution of that information. Corporate organisations would not be aware that their employees have blogs and could be posting sensitive information about the organisations, staff within the organisation, practices within the organisation, etc. An additional security risk is that blogs are not necessary text based, they could include photos or multimedia which would add to the security risk.

From an attackers perspective, blogging as a social engineering technique has many advantages. An attacker has open access to a large volume of information via the Internet. This information can be easy to access and contain a richness of information including multimedia content, providing the hacker with invaluable information to utlise in a social engineering attack.

CYBER CYCLE OF SOCIAL ENGINEERING

The authors propose a framework that could be used to describe the issues regarding Virtual social engineering. This relates to:

Reconnaissance

In terms of social engineering, there are a number of possible methods, these relate to ways in which information can be obtained:

> *Virtual Reconnaissance*
>
> This type of reconnaissance would relate to infecting a machine with spyware or malicious code. Social Engineering is the means by which an infection could occur e.g. social engineering emails trying to cause the infection.
>
> *Physical Reconnaissance*
>
> This type of reconnaissance would relate to collecting information via electronic means. This type of attack would relate to analysing blogs, mailing lists, sending social engineering emails to elicit information.

Collect Information

Once the reconnaissance stage has been completed information would be collected via the attacker. The collation would be via automated transfer of data, via malicious code, spyware or retrieving information directly from blogs.

Build up Information

Over a period of time, information will be collated and trends of the information will be determined. Information links and connections would be developed.

Using the Information

After a period of time, the direct attacks would occur. These attacks could occur in a number of ways. The information could be used to undertake an identity theft attack, that is using the information to obtain a virtual or physical personality and using that for another aim e.g. financial gain or physical fraud. Another way that the information could be used is to assume an identity and try to gain information from an organisation, e.g. someone assuming the online identity of a Corporate Information Officer and then using that identity to try and obtain information from actual employees from within the organisation.

CONCLUSION

The truth is that there is no technology in the world that can prevent a social engineering attack (Mitnick, 2002).

Social Engineering is changing the face of hacking activities. The concept of what social engineering was in the past has made a dramatic turn from being used in the physical environment to being prominent in the cyber environment. As we have seen in many examples reported by the media, it is clear that identity and information theft will become the most common and prolific future issue to affect individuals and organisations.

It will be the education of users and perhaps the unfortunate outcome of less social trust that will slow the pace of the social engineering hackers.

REFERENCES

Boslego, J. (2005), "Engineering social trust: what can communities and institutions do?", Harvard International Review, 27.1, p28.

Clyde L (2004) "Weblogs are you serious", The Electronic Library, Vol 22, No 5, Emerald Group Publishing.

Denning, D.E. (1999). "Information Warfare and Security", Addison Wesley, Reading: Mass.

Fialka, J. (1997). "War by other means: Economic Espionage in America", W.W.Norton & Company Inc, New York: London.

Finn T, Ding L, Zhou L and Joshi A (2005) "Social networking on the semantic web", The Learning Organisation, Vol 12, No 5, Emerald Group Publishing.

Gulati, R. (2003) "The Threat of Social Engineering and Your Defense Against It", SANS Reading Room. 2003. GIAC Security Essentials Certification Practical Assignment, SANS Institute, USA.

Mitnick K,(2002), "The Art of Deception: Controlling the Human Element of Security", Wiley, ISBN: 0-471-23712-4.

Rothkopf, D.J. (1999). "The Disinformation Age", Foreign Policy, 114, 82-96.

Turner, J.H. (2001), "Social Engineering: Is this really as bad as it sounds?", Sociological Practice: A Journal of Clinical and Applied Sociology, Vol. 3, No. 2.

Schwartau, W. (1996). "Information Warfare – second edition". Thunder's Mouth Press, New York.

Vijayan, J. (2005), "Targeted Attacks Pose New Security Challenge", Computerworld, Vol 39, No 26.

Warren M.J and Hutchinson W (2001) "Deception: A Tool and Curse for Security Management", IFIP/SEC 2001, 16th International Conference on Information Security, Paris, France.

Woolford, D. (1999) "Electronic Commerce: It's all a matter of trust", Computing Canada, 25:18, 13-15.

COPYRIGHT